EMT AKADEMİ

BİLGİSAYAR ADLİ İNCELEMELERİ

ADLİ BİLİŞİM ve ELEKTRONİK KEŞİF (E-DISCOVERY / E-KEŞİF) YÖNTEMLERİ

Serkan KÜÇÜK
Genel Müdür Yardımcısı
EMT Elektronik

Gazi Üniversitesi Fizik (BSc) ve Anadolu Üniversitesi İşletme (BBA) lisanlarını tamamlayan Serkan KÜÇÜK; 2000'li yılların başından itibaren Bilişim Suçları, Adli Bilişim ve Sayısal Veri İnceleme konularında çalışmaktadır.

Bilgisayar Sistemleri ve Mobil Cihazların adli veri incelemesi konularında dünyadaki sayılı yetkili eğiticilerden biridir, yurtiçinde ve yurtdışında özel şirketlere ve kolluk kuvvetlerine çok sayıda eğitim vermiş ve danışmanlık yapmıştır.

Alanında tüm dünyada büyük saygı gören yirmiye yakın sertifikaya sahip olan Serkan KÜÇÜK, uzun süre Ankara mahkemelerinde bilirkişi hizmeti vererek birçok önemli dosyanın çözümüne katkıda bulunmuştur.

Halen EMT Elektronik Ltd.'de Genel Müdür Yardımcılığı görevini yürütmektedir.

Adli veri incelemelerinde farklı yöntemlerin olduğundan daha önce bahsetmiş ve bunlardan triyaj (triage) yöntemi konusunda daha önce bir yazı hazırlamıştık. Bu yazıya aşağıdaki bağlantıdan ulaşabilirsiniz.
Triage.pdf

Bu yazımızda ise sıklıkla birbirine karıştırılan adli bilişim ve elektronik keşif (e-discovery / e-keşif) yöntemleri üzerinde duracağız.

Konunun daha anlaşılır olması açısından; kurumların projelerine ve planlamasına rehberlik etmek için avukatlar, yargıçlar, kurum içi danışmanlar ve diğer hukuk uzmanlarından oluşan EDRM isimli küresel danışma konseyinin yayınladığı e-keşif referans modeline aşağıdaki bağlantıdan ulaşabilirsiniz.
EDRM-clean-poster.pdf

Temel olarak hem adli bilişim hem de e-keşif uygulamalarında benzer adımlar takip edilir.
Bu adımlar sırası ile;

IDENTIFICATION (Tanımlama):

Potansiyel delil/bulgu kaynaklarının ve inceleme boyutunun belirlenmesi.

COLLECTION- PRESERVETION (Veri toplama ve koruma):

Potansiyel delil/bulgu kaynaklarından verilerin uygun şekilde toplanması ve herhangi bir değişikliğe ya da bozulmaya karşı korunması.

PROCESSING – REVIEW – ANALYSIS (Verileri İşleme – Gözden geçirme ve Analiz Etme):

Toplanan verilerin amaca uygun olarak işlenmesi, indekslenmesi, incelenmesi ve gerekli analizlerin yapılması.

PRODUCTION (Üretim):

İnceleme sonuçların uygun şekilde hazırlanması ve ilgililere teslim edilmesi.

PRESENTATION (Sunum):

İnceleme sonuçların doğru ve anlaşılır şekilde gösterilmesi.

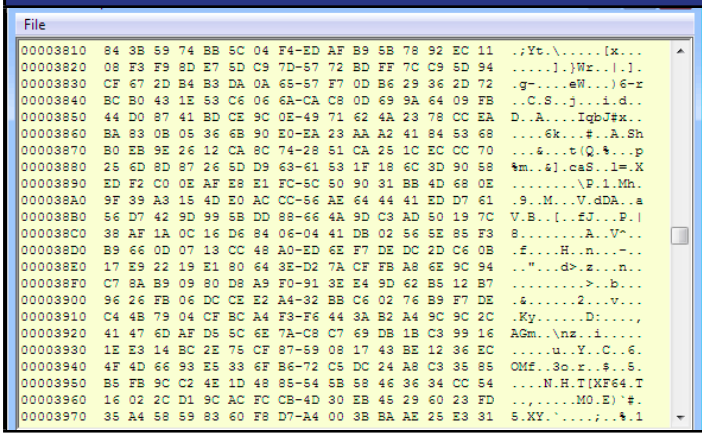
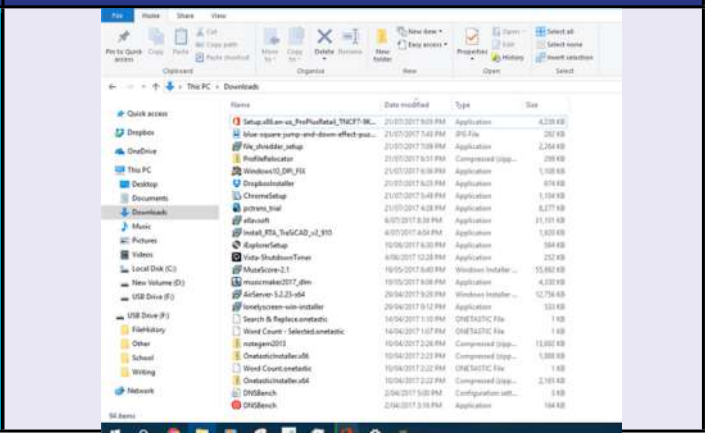
Adli bilişim ve e-keşif uygulamaları arasındaki temel fark ise e-keşif uygulamalarında belli bir veri kümesinin yukarıda açıklanan adımlar için seçilmesidir. Bu veri kümesi genellikle sadece ofis dosyalarıdır. (dokümanlar, hesap dosyaları, sunumlar, veri tabanları, pdf dosyaları, e-posta dosyaları, vs.)

Adli bilişim uygulamalarında ise belirlenen elektronik ortam ve/veya bilişim sistemlerinden veriler bit-by-bit (yani veriler ikilik tabanda en küçük veri depolama boyutu olan bit seviyesinde (0 ve 1) olacak kadar derinlemesine) kopyalanarak incelenir.

Örneğin, bir e-keşif uygulamasında 1TB kapasitesindeki bir sabit sürücüden sadece 10GB büyüklüğünde bir veri kümesinin incelenmesi yeterli olabilir. Fakat adli bilişim uygulamalarında ilk sektörden son sektöre kadar sabit sürücü içerisindeki tüm veriler incelenir. Dolayısı ile e-keşif, aslında adli bilişim incelemelerinin bir alt kümesidir diyebiliriz.

Aşağıdaki tabloda her iki yöntem için temel farklar yer almaktadır.

Adli Bilişim	E-Keşif
Sürücü (HDD) üzerindeki tüm veriler ile ilgilenir.	Sürücü (HDD) üzerindeki belli bir kısmi veri ile ilgilenir.
Tahsis edilmiş ve tahsis edilmemiş alanlarda inceleme yapılır. (PHYSICAL)	Sadece tahsis edilmiş alanlar üzerinde İnceleme yapılır. (LOGICAL)
Tüm dosyalar (silinmiş dosyalar, parçalı olarak üzerine yazılmış dosyalar, log dosyaları, vs.) önemlidir.	Programlar, geçici dosyalar, sistem dosyaları, vs. çok önemli değildir.
Sadece belli dosyalar değil, diğer kalıntılar da (internet geçmişi, chat mesajları, sisteme takılmış harici sürücüler, yüklenen programlar, açılan dosyalar, vs.) önemlidir.	Genellikle sadece ofis dosyaları (dokümanlar, hesap dosyaları, sunumlar, veri tabanları, pdf dosyaları, e-posta dosyaları, vs.) önemlidir.

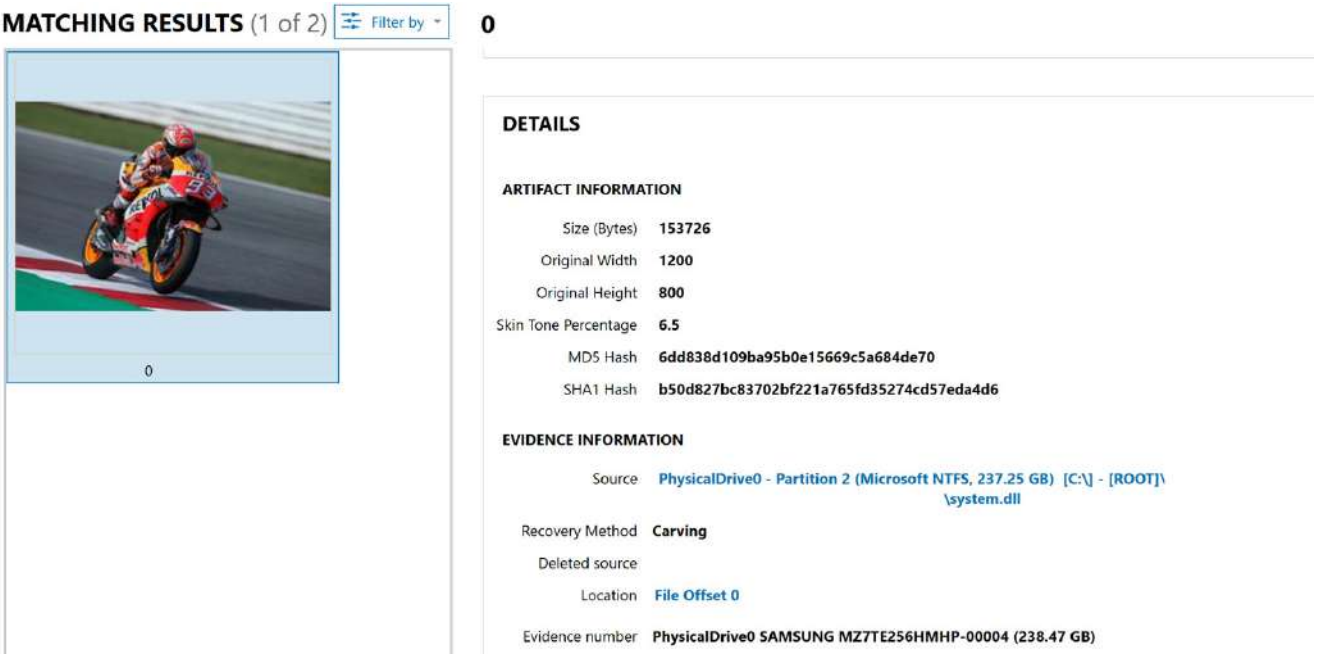
Adli Bilişim Yöntemi ile Görülen Veri	E-Keşif Yöntemi ile Görülen Veri
	

Örnek:

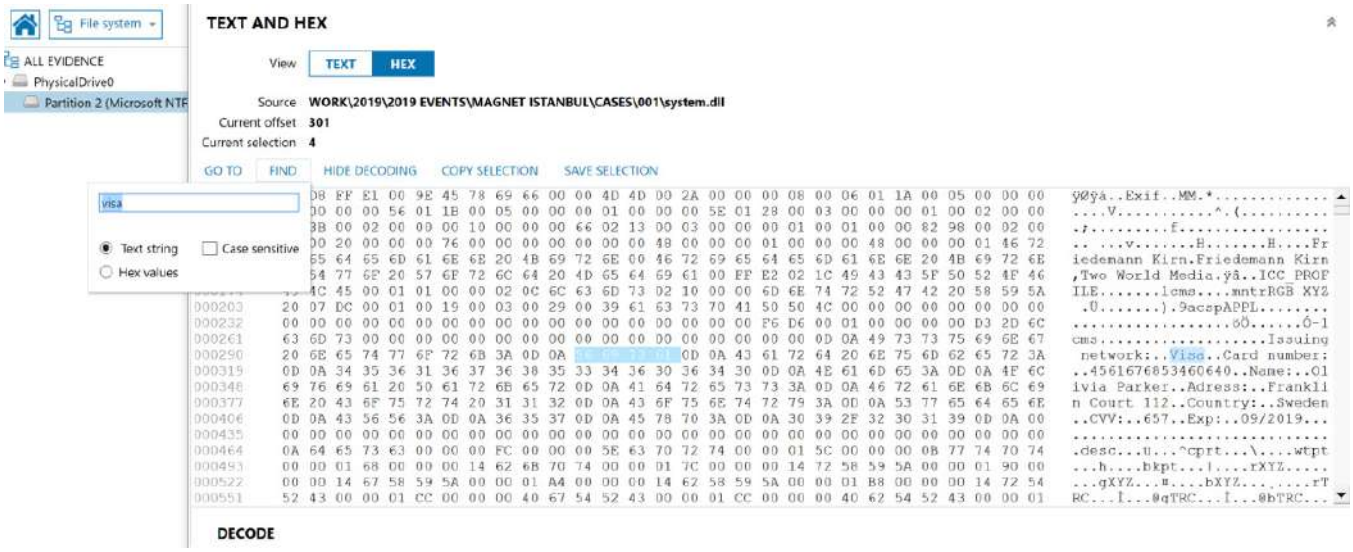
Bir Windows işletim sisteminde aşağıdaki dosya yer alıyor. (Silinmemiş bir dosya olduğunu kabul ediyoruz)

E-Keşif yöntemi ile yapılacak bir incelemede büyük ihtimal ile bu dosya görmezden gelinecektir, çünkü işletim sistemi bize bu dosyanın bir DLL dinamik bağlı kitaplık (dynamic link library) dosyası olduğunu göstermektedir. Genellikle sistem dosyaları e-keşif inceleme yönteminde pek dikkate alınmaz.

Fakat, adli bilişim yönetiminde işletim sistemlerinin bize neyi gösterdiği (veya göstermediği) önemli değildir. Adli bilişim yazılım ve donanımları alınan tüm verileri kendileri işleyerek ve değerlendirerek sunar. Aynı dosyayı, adli bilişim uzmanı aşağıdaki şekilde görecektir.



Aslında “system.dll” dosyası bir resim dosyası. Bunun nedeni ise kullanıcının dosya ismini değiştirmesi.
Peki kullanıcı neden bu dosyanın ismini değiştirmiş olabilir? Daha yakından bakalım…



Anlaşılan kullanıcı başkasına ait bir kredi kartı numarasını bu resmin içine saklamış ve bunun farkına varılmaması için dosyanın ismini değiştirmiş.

Not: Görsel de yer alan kredi kartı numarası sahtedir ve https://ccardgenerator.com/generat-visa-card-numbers.php adresinden oluşturulmuştur.

Adli bilişim yazılım ve araçları doğrudan fiziksel veriler üzerinde işlem yapabildiğinden, incelemeci tüm veri üzerinde bir arama (örneğin: "visa" kelimesini) yaptığında yukarıdaki sonuçlara ulaşabilecektir. Söz konusu veri silinmiş dahi olsa bile… Dahası bu dosyanın ne zaman, nereden, hangi kullanıcı tarafından; hangi yolla elde edildiği, oluşturulduğu, değiştirildiği, görüldüğünü belirlemek adli bilişim yöntemleri ile mümkündür.

SONUÇ:

Her iki yöntemde burada anlatılanlardan çok daha kapsamlıdır, incelemelerde amaca yönelik olarak farklı yaklaşımlar ve metodolojiler kullanılmaktadır. Uluslararası kabul gören yöntemlerle verilerin toplanması ve değerlendirilmesi gereklidir.

Yukarıda bahsedildiği üzere e-keşif yöntemi ile önemli deliller/bulgular toplanmayabilir (örneğin, silinmiş veya artık alanlardan elde edilebilecek önemli veriler). Dolayısı ile triyaj çalışmalarında olduğu gibi e-keşif incelemelerinde de dikkatli davranılmalı ve hiçbir zaman tam bir inceleme yerine geçebileceği düşünülmemelidir.

EK:

Örneğimiz de silinen verilerin aslında silinmediğinden bahsettik. Verilerin silinmesi konusunda Kişisel Verileri Koruma Kurumu (KVKK) tarafından yayınlanan rehberi aşağıdaki linkten inceleyebilirsiniz.
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

Verilerin tamamen yok edilmesi ise; verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Bunun için yerel sistemlerde "De-manyetize Etme" , "Fiziksel Yok Etme" ve "Üzerine Yazma" (Wipe) yöntemleri kullanılmaktadır. Bu konu ile ilgili detaylı bilgilere aşağıdaki sayfadan ulaşabilirsiniz.
https://www.emt.com.tr/tr/cozumler/guvenli-veri-imha-cozumleri-15

EMT Elektronik Mühendislik San. Tic. Ltd. Şti.
Çamlıca Mah., Anadolu Blv., No: 16
Regnum Tic. Merkezi, B Blok, No: 5/1
06200 Yenimahalle, Ankara - TÜRKİYE
+90 (312) 472 20 60
emtakademi@emt.com.tr
www.emt.com.tr